International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 7, Issue 1, Feb 2017, 53-58

TRANS STELLAR
•Journal Publications •Research Consultancy

A FRAMEWORK FOR KEEPING DATA SAFE IN CLOUD TRANSMISSIONS

D USHA

Assistant Professor, Department of Computer Science, Mother Teresa Women University, Kodaikanal, Tamilnadu, India

ABSTRACT

Cloud Computing is the generation architecture of Entreprises. The data is transferred between the client and server in cloud computing. Cloud computing contrasts traditional solutions with logical and physical controls. It moves the control to large data Centres with databases and application management software which may not dependable. Cloud security is significant in the current IT scenario. The uniqueness of the cloud also poses many security challenges which need more understanding. This paper focuses on cloud data storage and transmission security, which is an important parameter in the quality of service (QOS) of a cloud computing environment. To ensure faultlessness in user's cloud data an effective and flexible scheme different from antecedents is required [1]. Cloud storage allows users to store their data remotely and enjoy high quality applications on-demand without problems in hardware or software. The barriers in cloud data storage security is explored and an attempt is made to provide a trustworthy environment in cloud computing. This paper attempts to secure data without disturbing the network layers and protects the data from unlawful access into the server. The data is security is given high priority based on a user's choice of security methods.

KEYWORDS: Cloud, Private Cloud, Cloud Security, Protected Data Transmission & Network Layers

Received: Jan 02, 2017**; Accepted:** Jan 30, 2017**; Published:** Feb 02, 2017**; Paper Id.:** IJCSEITRFEB20176

Original Article

INTRODUCTION

Cloud computing is a recent phenomenon in IT where data is stored in data centres instead of desktops. The cloud infrastructure's hardware and system software provide the service and the applications are delivered over the internet. This sharing of resources reduces the cost to individuals. Cloud can be defined as a large pool of accessible resources which can be dynamically reconfigured to adjust load flexibility allowing optimum utilization [2]. Many Internet-based developments for Cloud Computing are opening up. The presence of broadband and wireless networking, declining storage costs and Internet computing software are the main driving forces behind cloud computing. Technical support from cloud infrastructures include virtualization, grid computing, service-oriented software, power efficiency and large facilities. The pioneers of Cloud Computing vendors are Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [1]. Online services provide huge amounts of storage space and customized computing resources eliminate local machines for data maintenance needs. However, users have to depend on cloud service providers for the availability and integrity of their data. Data security is an important aspect of QOS in the cloud and poses security threats for a number of reasons. Cryptography in data security protection cannot be directly in Cloud Computing as users may lose control of data. Since, different kinds of data of users is stored in the cloud, there exists a demand for assurances on their data safety. Verifying precision in cloud data becomes a challenging task. Moreover, Cloud Computing is not a data warehouse as the cloud data may updated frequently by users.

The construction has to reduce the communication overhead in comparison with replication techniques. A distributed data storage in Cloud Computing with a secure data transmission is attempted in this paper. The key features being quickness, location independence, reliability and maintenance. Figure 1 depicts the cloud computing general structure.

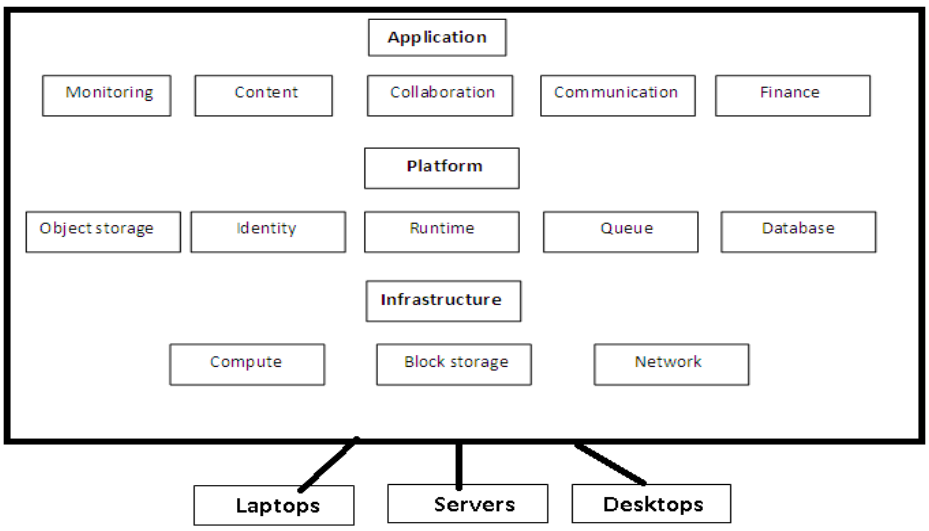

Figure 1: Clod Computing Structure

SYSTEM

Three network objects can be identified. Users who can be organizations or individuals. Users data for data computation is stored in the cloud. Cloud Service Provider (CSP) with resources manage cloud storage. Third Party Auditor (TPA) with expertise who expose risk of cloud storage services upon request [1] and [3]. Figure. 2 depicts the representative network architecture for cloud data storage

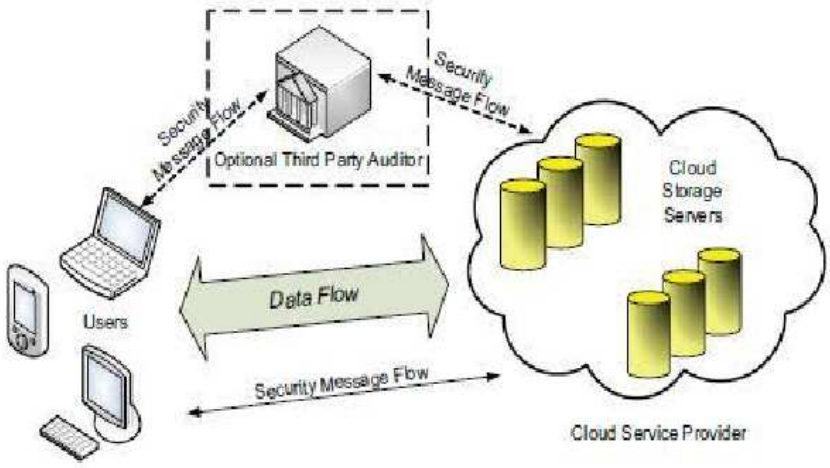

Figure 2: Data Storage Architecture in a Cloud

Any user stores the data through a CSP in cloud servers, running simultaneously. The user then interacts with the CSP servers to access data. This paper assumes a point-to-point communication channel exists between each cloud server and each user and that the user is reliable and authenticated. Security threats in cloud data storage can be viewed from two

angles. A CSP may not be trustworthy or malicious. CSPs may move the data that is rarely accessed to a lower tier of or attempt to hide a data loss incident due to management errors or failures. Challengers to cloud storage security may sometimes be robust or. The users' data may be deleted unknown to the CSPs. A feeble challenger may corrupt data files stored on individual servers and when the server is comprised they spoil the original data files by modifying or introducing fraudulent data. A robust challenger may compromise all the storage servers to intentionally modify the data files till they are internally consistent making all servers collude together to hide data loss or corruption. The aim of any data storage privacy has to be Storage accuracy for ensuring users data is stored appropriately, Identifying data errors locally or successfully identifying a malfunctioning server on data corruption, maintaining support dynamically by maintaining the same level of storage accuracy on user file updates, make data available in the midst of malicious data modifications server collusion to minimize the data failure effect and allow users to perform storage correctness checks.

ARCHITECTURES FOR CLOUD SECURITY

Many studies have studied different aspects of security in terms of problems and threats in cloud security and issues of virtualization security. Design of security architectures have also been proposed in previous studies. Cloud security research initiatives of HP, IBM, and Microsoft have been described [4]. Cloud computing has many security risks. HP research focuses on prototyping cells as a service to automate security management in cloud, where a cell is single administrative domain with security policies for virtual machines and storage volumes. IBM does a virtual machine introspection layering security inside a protected Virtual Machine running on same machine, employing protective methods as kernel functions and reducing running virus scanners. Microsoft protects the user data with a cryptography format for stored clouds, which the provider cannot get nor get to know details on the data. A secure virtualization technique called Advanced Cloud Protection System (ACPS) for ensuring security at a virtual machine manager level was proposed [5]. A guest user of one OS may interact with other Guest Oss in the cloud leading to a possible attacker or malicious connection. The ACPS can prevent unnecessary logins and maintain security of Oss with feeble passwords or SSH. Research on Data Storage security with respect to QOS was discussed [6]. The work proposed checking a data for attacks or integrity loss on the cloud. A homomorphism token similar to a hash function was generated to ensure that the data was not lost. It enabled a fast recovery of data after attacks or storage errors. It helped ensuring confidentiality and storage security of data in the cloud. There are issues in secure data transmission between a cloud Provider, a service provider and a cloud User. Secure data transmission achieved by protocols like SSL and IPSec which are used on the web and web applications can help secure cloud data transmissions. Secure data transmission was also designed for storage networks in [7] by developing Middleware below the application layer and selecting an appropriate security approach based available data clusters of an application.

It was proved to more secure than IPSec. A secure data transmission in cloud computing using transport layer techniques over the client and server was proposed in [8], The socket programming was applied to key exchanges to secure data over cloud and a comparison was done on response and processing times

PROPOSED CLOUD SECURITY FRAMEWORK

The proposed architecture is designed for private clouds and depicted in Figure 3. The novel security framework acts at the session layer but transparent to other layers. The client is secured first by authentication protocols and saved at the server. The data is securely stored in the server and any access or view of data is through the framework. This is executed at the application level to secure the data before transfer and other layers are not disturbed. The nodes are

connected to server using the security framework. When an Application user wants to send data to the cloud, a Security Algorithm based on the privacy level of the user document is chosen and for greater security, a robust security algorithm is chosen. The server saves the document in a database. All networked systems fall within the architectural limits. On a user document retrieval, the user has to connect to the same server where the document was saved, thus ensuring privacy for the user.

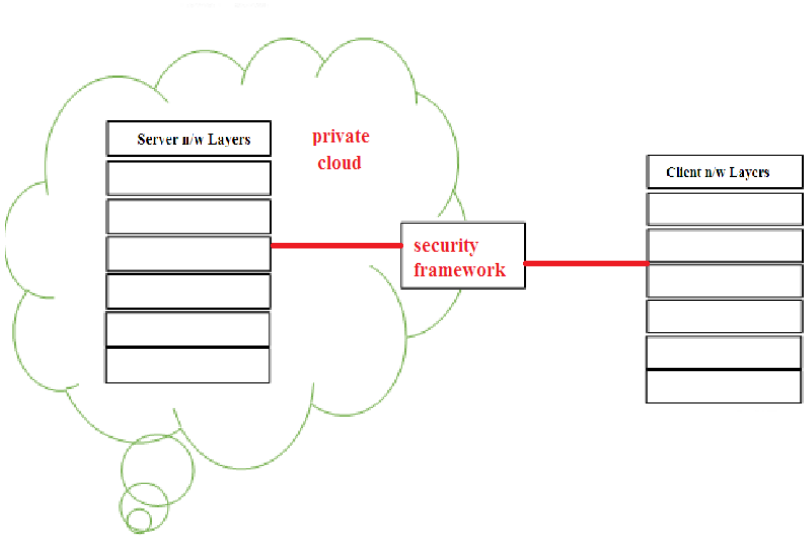

Figure 3: Secure Data Transmission Framework Architecture

Process While Storing a Document

The data of an initiator (client), encrypts the data using a key combination of the user's date of birth and a short name known only to the user and sent to the server. At the socket level the user's data is encrypted byte by byte with the key generated by the user and sent. The encrypted data is carried using protocols in the network. On the server the data or file is stored and an entry maintained in the database with the filename, username and the security key which is then passed on to the security framework. The process is depicted in Figure. 4.

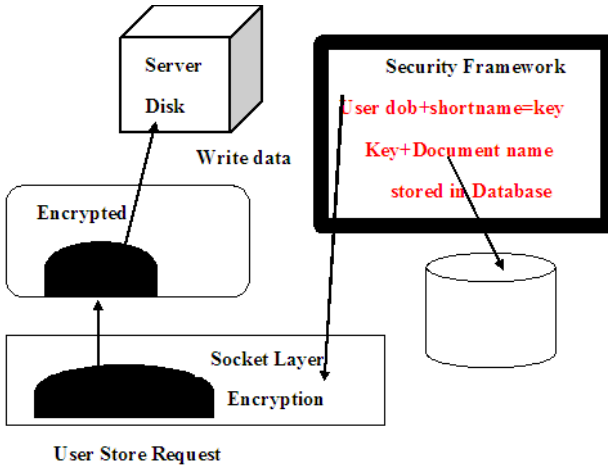

Figure 4: Encrypted Data Transmission and Store

Standard errors are obtained from a re-estimated model with no intercept. It can be noted in cross-section specific constant regression model estimations, multiple cross-section units take a longer time for estimations that are inaccurate

than those obtained using a fixed-effects option.

PROCESS WHILE RETRIEVING A DOCUMENT

The data for a user's document is accessed with the key generated by the user. The framework then checks the key with the document name and allows access to the document. After the authentication the encrypted document is transferred on the network and decrypted at the socket level of the client, ensuring safe transmission. The process is depicted in Figure. 5.

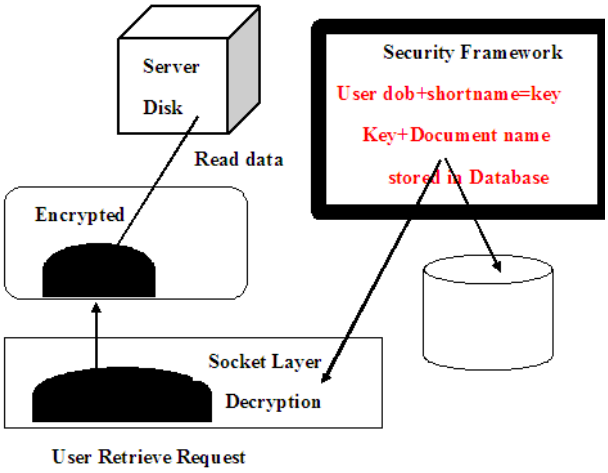

Figure 5: Encrypted Data Transmission and Retrieve

CONCLUSIONS

This paper investigated the problem of data security in cloud data storage during data transmissions. To ensure correctness of users' data in cloud data storage and avoiding data leakages during transmissions, a flexible user based encryption technique used by the framework was proposed. This framework can achieve data integration and security even at the server, since the data does not get decrypted till it reaches the client socket and can be decrypted with a key known only to the user, thus ensuring maximum security in transmissions and storage. The encryption key is highly efficient and resilient to malicious attacks. Since the files are encrypted and stored on the server, using the proposed cryptographic solution and with a user based encryption technique for the files to be accessed will work as a better approach to users for ensuring their data's security.

REFERENCES

1. *Cong Wang, Qian WangKui Ren, Ning Cao, and Wenjing Lou "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE transactions on services computing, vol. 5, no. 2, april-june 2012*
2. *Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, "A Break in Clouds: Towards a cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009, pp. 50-55.*
3. *Qian Wang,Cong Wang, Kui Ren, Wenjing Lou Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011*
4. *Gary Anthes, "Security in the cloud," In ACM Communications (2010), vol.53, Issue11, pp. 16-18.*

5. *Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.*
6. *Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1-11.*
7. *Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com, 2008.*
8. *Sudha.M, Bandaru Rama Krishna rao, M.Monica, "A Comprehensive approach to ensure secure data communication in cloud environment" International Jornal Of computer Applications, vol. 12. Issue 8, pp. 19-23.*